Math. Proc. Camb. Phil. Soc. (2012), **152**, 571 © *Cambridge Philosophical Society* 2012
doi:10.1017/S0305004111000399

CORRIGENDUM

Pseudoprime Reductions of Elliptic Curves – CORRIGENDUM

BY ALINA CARMEN COJOCARU, FLORIAN LUCA and IGOR E. SHPARLINSKI

doi: 10.1017/S0305004108001758, Published by Cambridge University Press, 14 July 2008.

Unfortunately, there are two inaccuracies in the argument of [**CLS**]. First, the statements of Lemmas 3, 4, 6, and 7 of [**CLS**] hold only under the additional condition $\gcd(m, M_E) = 1$ for some integer $M_E \geqslant 1$ depending only on E. Second, the divisibility condition (3·6) in [**CLS**] implies that $t_b(\ell) \mid n_E(p) - 1$ (rather than $t_b(\ell) \mid n_E(p)$, as it was erroneously claimed on p. 519 in [**CLS**]). In particular, instead of the divisibility $\ell t_b(\ell) \mid n_E(p)$ (see the last displayed formula on p. 519 in [**CLS**]), we conclude that for every prime $\ell \mid L$ there is an integer a_ℓ such that

$$n_E(p) \equiv a_\ell \pmod{\ell t_b(\ell)}. \tag{0·1}$$

However, the final result is correct and can easily be recovered. To do so, we remark that under the condition $\gcd(m, M_E) = 1$, we have full analogues of Lemmas 6, 7, 9, and 10 of [**CLS**] for the function $\Pi(x; m, a)$ defined as the number of primes $p \leqslant x$ with $n_E(p) \equiv a \pmod{m}$ (rather than just for $\Pi(x; m) = \Pi(x; m, 0)$ as in [**CLS**]). Define $\rho^*(n)$ as the largest square-free divisor of n which is relatively prime to M_E. We then derive from (0·1) above that

$$n_E(p) \equiv a_\ell \pmod{\ell \rho^*(t_b(\ell))}.$$

Therefore

$$\#\mathcal{T} \leqslant \sum_{y<\ell\leqslant z} \Pi(x; \ell\rho^*(t_b(\ell)), a_\ell). \tag{0·2}$$

Since

$$\rho^*(n) \mid \rho(n) \qquad \text{and} \qquad \rho^*(n) \geqslant \rho(n)/M_E,$$

we see that (0·2) above implies the bound (3·7) from [**CLS**], and the result now follows without any further changes.

The authors are grateful to Chantal David and Jie Wu for pointing out these inaccuracies to them. They have also recently found some slight improvements of the estimates from [**CLS**] and more substancial improvements under an additional assumption (see [**DW**]).

REFERENCES

[**CLS**] A. C. COJOCARU, F. LUCA and I. E. SHPARLINSKI. Pseudoprime reductions of elliptic curves. *Math. Proc. Camb. Phil. Soc.* **146** (2009), 513–522.
[**DW**] C. DAVID and J. WU. Pseudoprime reductions of elliptic curves. *Can. J. Math.* **64** (2012), 81–101.